



INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : <b>G07F 7/10, H04L 9/00</b>	<b>A2</b>	(11) Internationale Veröffentlichungsnummer: <b>WO 98/39745</b> (43) Internationales Veröffentlichungsdatum: 11. September 1998 (11.09.98)
(21) Internationales Aktenzeichen: PCT/EP98/01269 (22) Internationales Anmeldedatum: 5. März 1998 (05.03.98) (30) Prioritätsdaten: 197 09 274.8 6. März 1997 (06.03.97) DE (71) Anmelder: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE). (72) Erfinder: HARTLEIF, Siegfried; Heinrich-Heine-Strasse 18A, D-64823 Groß-Umstadt (DE). SCHAEFER-LORINSER, Frank; Potsdamerstrasse 88, D-64372 Ober-Ramstadt (DE).	(81) Bestimmungsstaaten: HU, NO, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  Veröffentlicht <i>Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.</i>	

(54) Title: PORTABLE DATA CARRIER AND METHOD FOR CRYPTOGRAPHICALLY SECURE USE THEREOF WITH INTER-CHANGEABLE KEYS

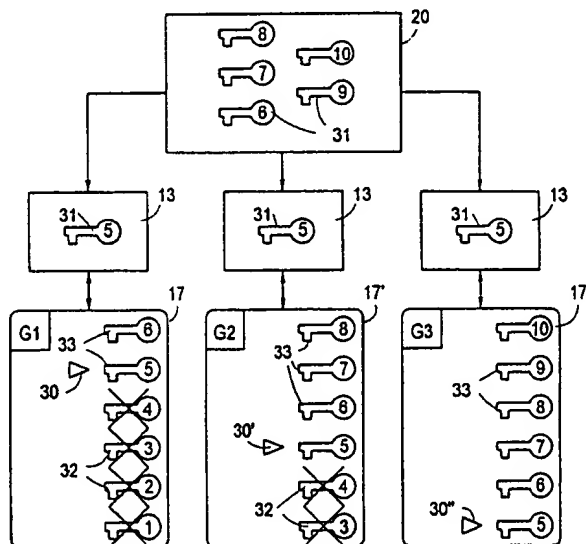
(54) Bezeichnung: TRAGBARER DATENTRÄGER UND VERFAHREN ZU DESSEN KRYPTOGRAPHISCH GESICHERTEN BENUTZUNG MIT AUSTAUSCHBAREN KRYPTOGRAPHISCHEN SCHLÜSSELN

(57) Abstract

The invention relates to a portable data carrier, especially a chip card, to store data in the form of data records, wherein cryptographic keys are memorized on the data carrier in order to protect the writing and reading of said data records. A series of keys is thus stored on the data carrier to perform this task. Means are provided to make the keys in the data carrier unfit for use. Also disclosed is a method for using a data carrier wherein the use of each key to read or write data is preceded by verification of whether the key is older than the key whose identification mark is stored on the data carrier. The use of said key is denied if the results of the verification are positive.

(57) Zusammenfassung

Bei einem tragbaren Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel auf dem Datenträger gespeichert sind, ist eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert. Es sind Mittel zur Unbrauchbarmachung von Schlüsseln im Datenträger vorgesehen. Es wird ein Verfahren zur Benutzung des Datenträgers angegeben, wobei vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel älter ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist. Bei positivem Ergebnis dieser Prüfung wird die Benutzung des Schlüssels abgelehnt.



# **LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Tragbarer Datenträger und Verfahren zu dessen  
kryptographisch gesicherten Benutzung mit austauschbaren  
kryptographischen Schlüsseln

Die Erfindung betrifft einen tragbaren Datenträger,  
insbesondere Chipkarte, zum Speichern von Daten in Form von  
Datensätzen, wobei zur Absicherung des Schreibens und Lesens  
der Datensätze kryptographische Schlüssel auf dem  
Datenträger gespeichert sind, sowie ein Verfahren zur  
Benutzung des Datenträgers.

Im täglichen Leben werden häufig Berechtigungen erworben;  
Beispiele dafür sind die Berechtigung zur Benutzung von  
Verkehrsmitteln oder Schwimmbädern. Auf sogenannten  
Chipkarten, die oft zur Abrechnung von Geldbeträgen  
verwendet werden, also zum Beispiel eine elektronische  
Geldbörse enthalten, werden heutzutage auch Berechtigungen  
in elektronischer Form gespeichert.

Damit stehen Mittel zur Verfügung, die ein umfassendes  
Abrechnungssystem ermöglichen, in dem mit Hilfe nur einer  
Chipkarte je Benutzer elektronische Berechtigungen benutzt  
werden, in dem mit elektronischem Geld bezahlt wird, und  
andere Transaktionen möglich sind.

Da die sichere Speicherung kryptographischer Schlüssel einen  
potentiellen Schwachpunkt bezüglich der Sicherheit eines  
solchen Systems darstellt, möchte man die Verwendbarkeit

...

eines Schlüssels zeitlich so eingrenzen, daß ein Betrug durch Mißbrauch von Schlüsseln aus Zeitgründen erschwert oder gar unmöglich wird. Daher stattet man zum Beispiel in regelmäßigen Abständen neu ausgegebene Chipkarten mit neu gewählten Schlüsseln aus. Die mit den Chipkarten kommunizierenden Sicherheitsmodule in den Endgeräten des Systems, die aus Kostengründen nur zeitweilig mit den diversen Verrechnungsstellen verbunden sind und in der restlichen Zeit selbständig arbeiten, müssen in diesem Fall jedoch über mehrere Generationen von Hauptschlüsseln verfügen, um alle gültigen Karten unterstützen zu können.

Falls kein extrem hoher physikalischer Schutz der Sicherheitsmodule gegeben ist, stellen die langlebigen Hauptschlüssel in den Sicherheitsmodulen selbst einen sicherheitstechnischen Schwachpunkt dar.

Der Erfindung liegt nun die Aufgabe zugrunde, eine Änderung von möglicherweise aus Sicherheitsmodulen ausgespäteten Schlüsseln zu ermöglichen, ohne daß damit alle betroffenen Chipkarten ausgetauscht werden müssen. Im Falle eines Diebstahls von Hauptschlüsseln eines Sicherheitsmoduls muß es möglich sein, die entsprechenden Gegenstücke auf allen im Umlauf befindlichen Chipkarten unwirksam zu machen.

Erfindungsgemäß wird diese Aufgabe bei einem tragbaren Datenträger, insbesondere einer Chipkarte, dadurch gelöst, daß eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert ist und daß Mittel zur Unbrauchbarmachung von Schlüsseln im Datenträger vorgesehen sind.

Die Schlüssel werden im Normalfall eine bestimmte Zeit lang benutzt und auf Befehl einer Zentrale hin bei der nächsten Verwendung der Chipkarte unbrauchbar gemacht. Gleichzeitig erhalten alle Sicherheitsmodule neue Hauptschlüssel, passend

...

zu den auf den Chipkarten aktivierten neuen Schlüsseln. Diesen Befehl kann man auch dann geben, wenn der bloße Verdacht eines Betrugsversuchs besteht oder wenn ein Sicherheitsmodul gestohlen wurde. Ein potentieller Betrüger hat damit wenig Zeit, einen Betrug gewinnbringend auszuführen.

Eine erste Weiterbildung des erfindungsgemäßen Datenträgers besteht darin, daß als Mittel zur Unbrauchbarmachung ein Zähler vorgesehen ist, wobei jedem Schlüssel auf dem Datenträger ein Zählerwert zugeordnet ist, daß der Zähler nicht dekrementierbar ist und daß diejenigen Schlüssel unbrauchbar sind, deren Zählerwert kleiner als der Zählerstand ist. Es wird nun auf Befehl einer Zentrale hin bei der nächsten Verwendung der Chipkarte der Zähler inkrementiert und damit ist der bis dahin verwendete Schlüssel ungültig. Sämtliche Sicherheitsmodule werden mit neuen Hauptschlüsseln versorgt. Der Benutzer nimmt von dem Vorgang keine Notiz.

Eine andere Weiterbildung des erfindungsgemäßen Datenträgers sieht Speicherplatz vor zur Aufnahme eines Identifikationsmerkmals des zum Schreiben eines Datensatzes zuletzt verwendeten Schlüssels, beispielsweise des dem Schlüssel zugeordneten Zählerwertes. Bei einer dritten Weiterbildung ist vorgesehen, daß zu jedem Datensatz Speicherplatz vorgesehen ist, worin ein Identifikationsmerkmal desjenigen Schlüssels speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde. Diese Maßnahmen ergeben eine Kontrollmöglichkeit über die mit der Chipkarte zuletzt verwendeten Schlüssel - entweder für die gesamte Chipkarte oder für einzelne Datensätze, beispielsweise Berechtigungen.

...

Ein erfindungsgemäßer Vorgang, bei dem diese Kontrollmöglichkeit genutzt wird, ist bei dem erfindungsgemäßen Verfahren dadurch verwirklicht, daß vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel älter ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist und daß bei positivem Ergebnis dieser Prüfung die Benutzung des Schlüssels abgelehnt wird. So könnte man in dem Fall beispielsweise die betroffene Chipkarte aus dem Verkehr ziehen, da sie offenbar fehlerhaft oder für einen Betrugsversuch mißbraucht worden ist.

Damit der Wechsel von einem alten Schlüssel zu einem neuen reibungslos und automatisch vonstatten geht, ist es vorteilhaft, wie es eine Weiterbildung des erfindungsgemäßen Verfahrens vorsieht, daß vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob er neuer ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist, daß bei positivem Ergebnis dieser Prüfung das gespeicherte Identifikationsmerkmal durch eines des neueren Schlüssels ersetzt wird und daß alle älteren Schlüssel auf dem Datenträger unbrauchbar gemacht werden. Auf diese Weise werden die Schlüssel auf der Chipkarte nach und nach verbraucht, bis die Gültigkeitsdauer der Chipkarte abgelaufen ist und sie ungültig wird.

Bei einer anderen vorteilhaften Weiterbildung des Verfahrens ist vorgesehen, daß ein zu lesender Datensatz, insbesondere Berechtigungsdatensatz, der mit einem über ein vorgegebenes Maß veralteten Schlüssel geschrieben ist, verworfen wird. Damit läßt sich vermeiden, daß gefälschte Berechtigungen, die mit einem entwendeten älteren Schlüssel erstellt wurden, genutzt werden können.

...

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 ein Endgerät als Blockschaltbild sowie eine erfindungsgemäße Chipkarte,

Fig. 2 ein Berechtigungssystem,

Fig. 3 Schlüssel und Zähler erfindungsgemäßer Chipkarten und

Fig. 4 den Vorgang beim Überprüfen eines Schlüssels.

Gleiche Teile sind in den Figuren mit gleichen Bezugszeichen versehen.

Das Blockschaltbild gemäß Fig. 1 umfaßt ein Endgerät 11, das einen Prozessor 12, ein Sicherheitsmodul 13 und ein Karten-Schreib- und Lesegerät 14 enthält. Ferner ist eine Tastatur 15 vorgesehen für Eingaben durch einen Benutzer, falls solche erforderlich sind. Das Sicherheitsmodul 13 ist derart gestaltet, daß Daten- und Programmänderungen sowie ein Auslesen von Programmen und Daten nicht möglich sind. Die einzelnen Baugruppen des Endgerätes 11 sind durch Datenleitungen 16 miteinander verbunden. In das Schreib- und Lesegerät 14 kann eine Chipkarte 17 eingeführt werden.

In dem Berechtigungssystem gemäß Fig. 2, das erfindungsgemäße Chipkarten 17 benutzt, werden die Sicherheitsmodule 13 der Endgeräte 11 von einer physikalisch gesicherten Zentrale 20 aus über ein Telekommunikationsnetz 19 mit Hauptschlüsseln und anderen Informationen versorgt. Diverse Kontrollgeräte 21, 22, die immobile Anwendungen (Schwimmbäder, Telefone) bedienen, sind ebenfalls mit dieser Zentrale 20 verbunden. Andere Kontrollgeräte 23 bedienen

...

mobile Anwendungen, beispielsweise Buslinien 24, und arbeiten autark. Alle Abrechnungen, welche die Endgeräte 11 mit den Chipkarten 17 vornehmen, werden regelmäßig den Verrechnungsstellen 25 (z.B. Banken) mitgeteilt.

Fig. 3 zeigt, wie Schlüssel 32, 33 auf den Chipkarten 17, 17', 17'' unbrauchbar werden und wie die Sicherheitsmodule 13 mit neuen Hauptschlüsseln (Masterkey) 31 versorgt werden. Die Hauptschlüssel 31 sind entsprechend ihrer zeitlichen Gültigkeit durchnummeriert. Dazu passende Schlüssel 32, 33 auf den Chipkarten 17, 17', 17'' sind ebenfalls mit Nummern versehen, wobei die Schlüssel 33 zu dem mit jeweils gleicher Nummer versehenen Hauptschlüssel 31 passen. Die jeweils durch einen Pfeil symbolisierten Zähler 30, 30', 30'' werden beispielsweise jedes halbe Jahr inkrementiert, das heißt bei der ersten Benutzung nach diesem Zeitraum. Alle Schlüssel 32 mit einer kleineren Nummer als der Zählerstand, sind unwirksam und daher in der Figur durchgestrichen. Die Chipkarten 17, 17', 17'' haben eine Gültigkeitsdauer von drei Jahren, brauchen also jeweils sechs Schlüssel 32, 33. Jedes Jahr werden neue Chipkarten 17, 17', 17'' ausgegeben, so daß die neuen Chipkarten 17, 17', 17'' jeweils zwei neue Schlüssel 33 gegenüber der jeweils älteren 17, 17'' benötigen. Die Chipkarte 17 ist demnach etwa zwei Jahre alt, Chipkarte 17' ein Jahr und die Chipkarte 17'' ist neu. Es sind bei diesem Beispiel ständig drei Generationen G1, G2, G3 von Chipkarten mit insgesamt sechs unwirksamen und wirksamen Schlüsseln 32, 33 im Umlauf.

Wenn die Zentrale 20 einen neuen Hauptschlüssel 31 an die Sicherheitsmodule 13 verteilt, werden nach und nach die Zähler 30, 30', 30'' aller Chipkarten 17, 17', 17'' inkrementiert, sobald sie mit einem Sicherheitsmodul 13 kommunizieren. Auf diese Weise ist es ausgeschlossen, daß ein Betrüger mit dem Diebstahl eines Sicherheitsmoduls 13 in den Besitz aller Hauptschlüssel 31 kommt, die für die

...



aktuell gültigen Chipkarten 17, 17', 17" vorgehalten werden müssen. Er hat nur die Chance, einen einzigen Hauptschlüssel 31 (mit der Nummer 5) zu erbeuten. Innerhalb des halben Jahres, in dem der erbeutete Hauptschlüssel 31 gültig ist, läßt sich ein Betrug jedoch kaum gewinnbringend ausführen.

Das Flußdiagramm gemäß Fig. 4 zeigt die Anwendung eines Schlüssels, wobei nach einem Start bei 40 bei 41 der neue Schlüssel KN und bei 42 der alte Schlüssel KO gelesen werden. Bei 43 wird geprüft, ob der neue Schlüssel KN neuer als oder gleich alt wie der bis dahin verwendete alte Schlüssel KO ist. Ist dies nicht der Fall, wird die Operation bei 44 abgebrochen. Anderenfalls wird bei 45 geprüft, ob der neue Schlüssel KN neuer als der alte Schlüssel KO ist. Zutreffendenfalls wird im Schritt 46 KO auf KN gesetzt. In beiden Fällen wird bei 47 die Berechtigung A freigegeben.

...

## Ansprüche

1. Tragbarer Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel (32, 33) auf dem Datenträger (7) gespeichert sind, dadurch gekennzeichnet, daß eine Reihe von Schlüsseln (32, 33) für den jeweiligen Verwendungszweck auf dem Datenträger (7) gespeichert ist und daß Mittel (30) zur Unbrauchbarmachung von Schlüsseln (32, 33) im Datenträger (7) vorgesehen sind.
2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß als Mittel zur Unbrauchbarmachung ein Zähler (30) vorgesehen ist, wobei jedem Schlüssel (32, 33) auf dem Datenträger ein Zählerwert zugeordnet ist, daß der Zähler (30) nicht dekrementierbar ist und daß diejenigen Schlüssel (32) unbrauchbar sind, deren Zählerwert kleiner als der Zählerstand ist.
3. Datenträger nach einem der vorhergehenden Ansprüche, gekennzeichnet durch Speicherplatz zur Aufnahme eines Identifikationsmerkmals (42) des zum Schreiben eines Datensatzes zuletzt verwendeten Schlüssels (33), beispielsweise des dem Schlüssel (33) zugeordneten Zählerwertes.

...

4. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß in jedem Datensatz, insbesondere Berechtigungsdatensatz, Speicherplatz vorgesehen ist, worin ein Identifikationsmerkmal (42) desjenigen Schlüssels (33) speicherbar ist, mit dem der Datensatz zuletzt geschrieben wurde.

5. Verfahren zur Benutzung eines Datenträgers nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß vor jeder Benutzung eines Schlüssels (33) zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel (33) älter ist als derjenige, dessen Identifikationsmerkmal (42) auf dem Datenträger gespeichert ist und daß bei positivem Ergebnis dieser Prüfung die Benutzung des Schlüssels (33) abgelehnt wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß vor jeder Benutzung eines Schlüssels (33) zum Schreiben oder Lesen von Daten geprüft wird, ob er neuer ist als derjenige, dessen Identifikationsmerkmal (42) auf dem Datenträger gespeichert ist, daß bei positivem Ergebnis dieser Prüfung das gespeicherte Identifikationsmerkmal (42) durch eines (40) des neueren Schlüssels ersetzt wird und daß alle älteren Schlüssel (32) auf dem Datenträger unbrauchbar gemacht werden.

7. Verfahren nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß ein zu lesender Datensatz, insbesondere Berechtigungsdatensatz, der mit einem über ein vorgegebenes Maß veralteten Schlüssel geschrieben ist, verworfen wird und insbesondere die Berechtigung verworfen wird.

...

1/2

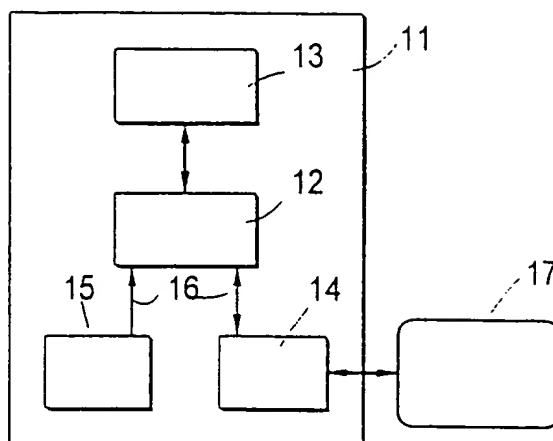


Fig.1

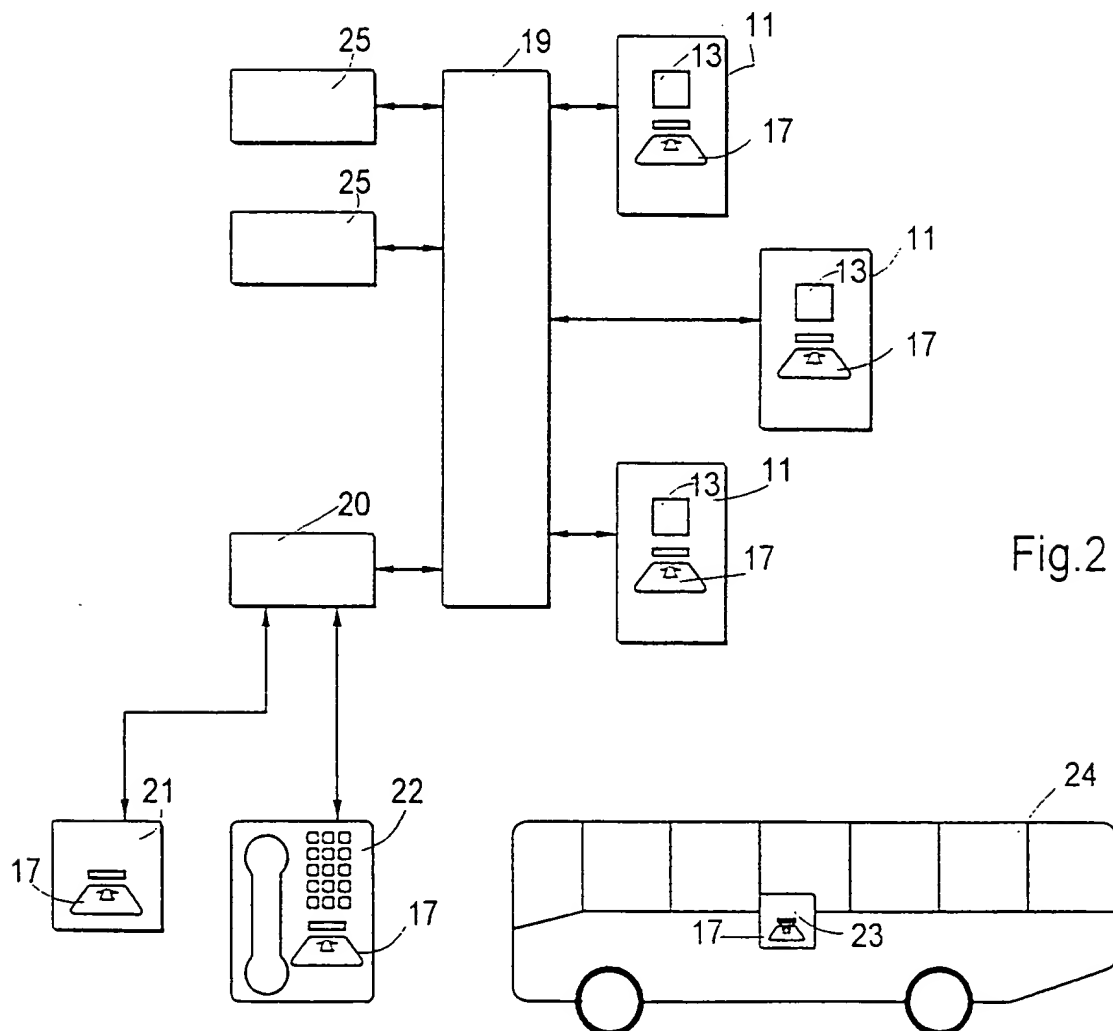


Fig.2

2/2

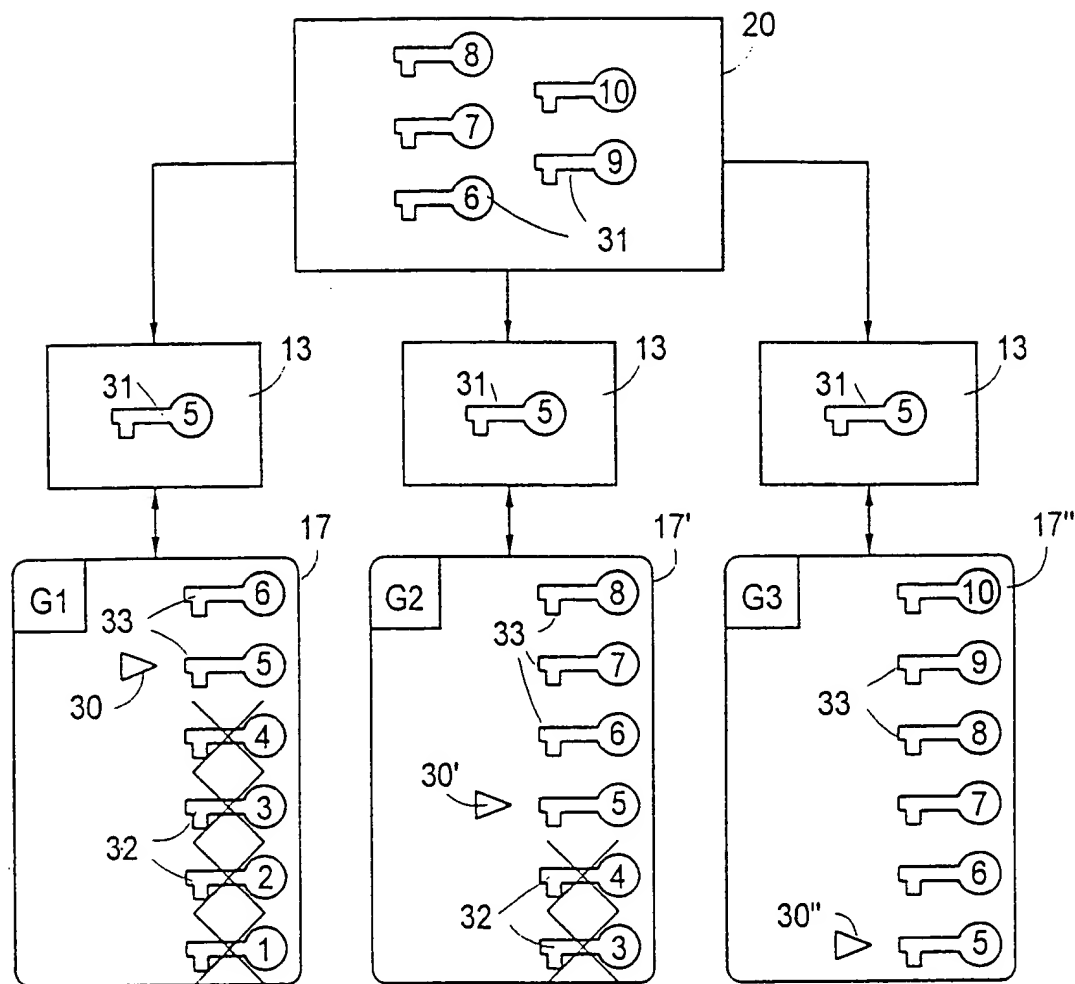


Fig.3

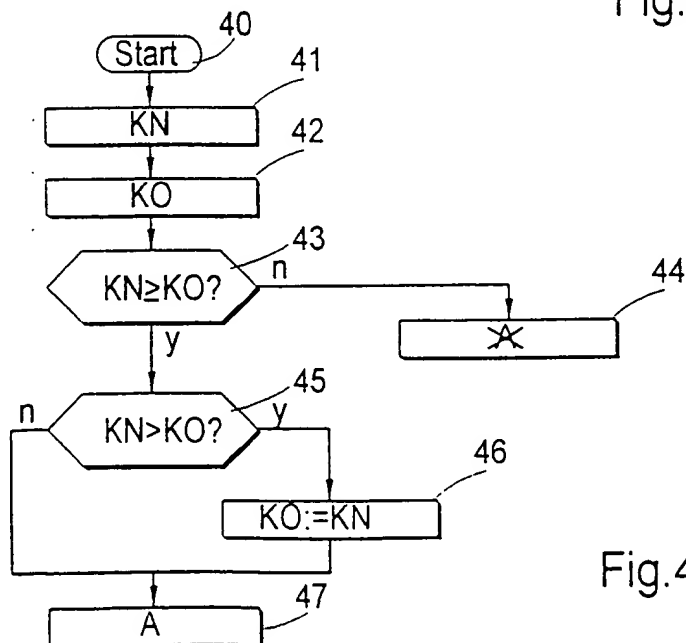


Fig.4



1/2

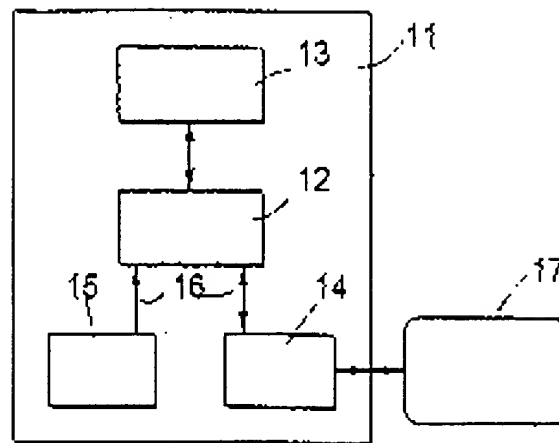


Fig. 1

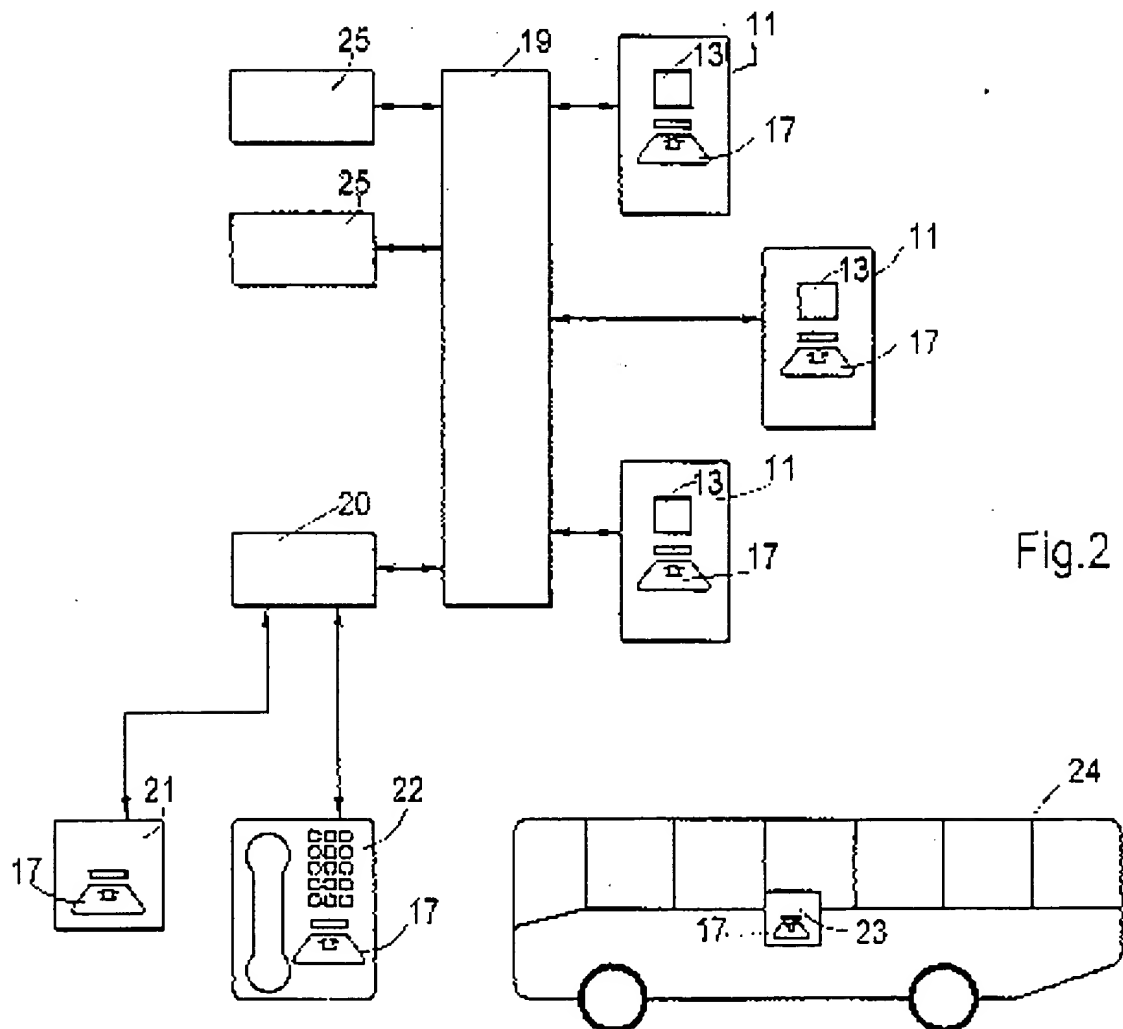


Fig. 2

2/2

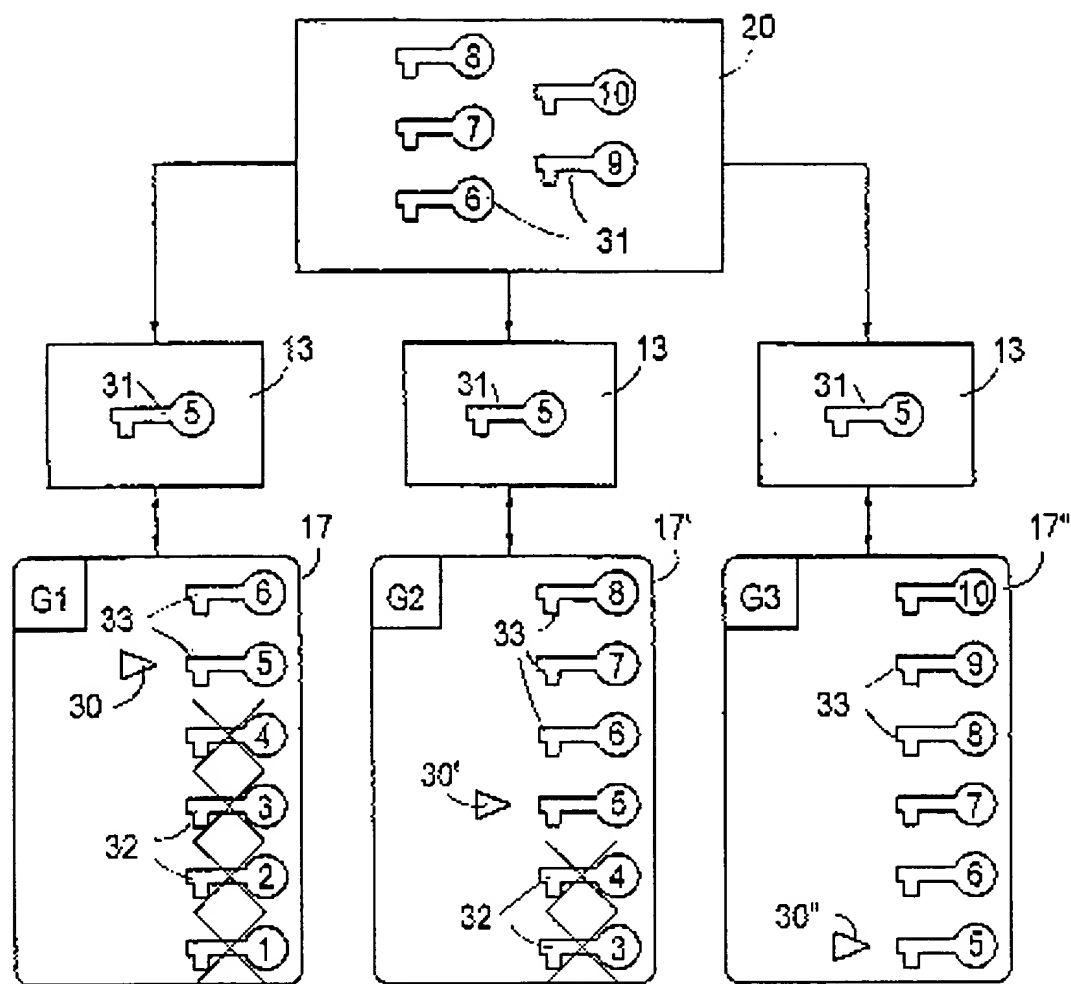


Fig. 3

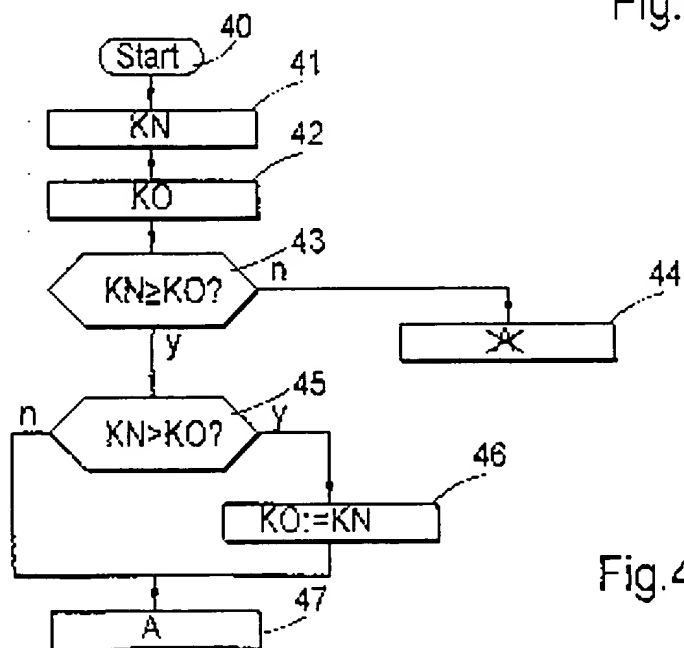


Fig. 4




 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation <sup>6</sup> : <b>G07F 7/10, H04L 9/00</b>		A3	(11) Internationale Veröffentlichungsnummer: <b>WO 98/39745</b>
		(43) Internationales Veröffentlichungsdatum:	11. September 1998 (11.09.98)
(21) Internationales Aktenzeichen: PCT/EP98/01269 (22) Internationales Anmeldedatum: 5. März 1998 (05.03.98) (30) Prioritätsdaten: 197 09 274.8      6. März 1997 (06.03.97)      DE (71) Anmelder: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE). (72) Erfinder: HARTLEIF, Siegfried; Heinrich-Heine-Strasse 18A, D-64823 Groß-Umstadt (DE). SCHAEFER-LORINSER, Frank; Potsdamerstrasse 88, D-64372 Ober-Ramstadt (DE).		(81) Bestimmungsstaaten: HU, NO, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht <i>Mit internationalem Recherchenbericht.          Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i> (88) Veröffentlichungsdatum des internationalen Recherchenberichts: 14. Januar 1999 (14.01.99)	
(54) Title: PORTABLE DATA CARRIER AND METHOD FOR CRYPTOGRAPHICALLY SECURE USE THEREOF WITH INTER-CHANGEABLE KEYS (54) Bezeichnung: TRAGBARER DATENTRÄGER UND VERFAHREN ZU DESSEN KRYPTOGRAPHISCH GESICHERTEN BENUTZUNG MIT AUSTAUSCHBAREN KRYPTOGRAPHISCHEN SCHLÜSSELN (57) Abstract <p>The invention relates to a portable data carrier, especially a chip card, to store data in the form of data records, wherein cryptographic keys are memorized on the data carrier in order to protect the writing and reading of said data records. A series of keys is thus stored on the data carrier to perform this task. Means are provided to make the keys in the data carrier unfit for use. Also disclosed is a method for using a data carrier wherein the use of each key to read or write data is preceded by verification of whether the key is older than the key whose identification mark is stored on the data carrier. The use of said key is denied if the results of the verification are positive.</p>			
(57) Zusammenfassung <p>Bei einem tragbaren Datenträger, insbesondere Chipkarte, zum Speichern von Daten in Form von Datensätzen, wobei zur Absicherung des Schreibens und Lesens der Datensätze kryptographische Schlüssel auf dem Datenträger gespeichert sind, ist eine Reihe von Schlüsseln für den jeweiligen Verwendungszweck auf dem Datenträger gespeichert. Es sind Mittel zur Unbrauchbarmachung von Schlüsseln im Datenträger vorgesehen. Es wird ein Verfahren zur Benutzung des Datenträgers angegeben, wobei vor jeder Benutzung eines Schlüssels zum Schreiben oder Lesen von Daten geprüft wird, ob der Schlüssel älter ist als derjenige, dessen Identifikationsmerkmal auf dem Datenträger gespeichert ist. Bei positivem Ergebnis dieser Prüfung wird die Benutzung des Schlüssels abgelehnt.</p>			

# LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 98/01269

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 G07F7/10 H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 681 165 A (GEMPLUS CARD INTERNATIONAL) 12 March 1993 see abstract; claims; figures ---	1,3
Y	US 4 605 820 A (C.M. CAMPBELL) 12 August 1986 see abstract; claims; figures 1,2,8 ---	1,3
A	---	2
A	US 4 731 840 A (S.M. MNISZEWSKI) 15 March 1988 see abstract; figures see column 3, line 44 - column 5, line 14 ---	1-4
A	WO 96 07994 A (BANKSYS) 14 March 1996 see abstract; claims; figure ---	1,2,4-7
A	GB 2 227 111 A (TOSHIBA) 18 July 1990 -----	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

**\* Special categories of cited documents :**

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

25 November 1998

Date of mailing of the international search report

02/12/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

David, J

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 98/01269

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2681165 A	12-03-1993	NONE	
US 4605820 A	12-08-1986	NONE	
US 4731840 A	15-03-1988	NONE	
WO 9607994 A	14-03-1996	BE 1008699 A AT 172805 T AU 687622 B AU 3377895 A CA 2199504 A EP 0780012 A NO 971066 A	02-07-1996 15-11-1998 26-02-1998 27-03-1996 14-03-1996 25-06-1997 09-05-1997
GB 2227111 A	18-07-1990	JP 2187888 A JP 2187785 A FR 2641885 A US 5293029 A	24-07-1990 23-07-1990 20-07-1990 08-03-1994

Form PCT/ISA/210 (patent family annex) (July 1992)

### In nationales Aktenzeichen

PCT/EP 98/01269

### A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 G07F7/10 H04L9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 G07F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

### C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	FR 2 681 165 A (GEMPLUS CARD INTERNATIONAL) 12. März 1993 siehe Zusammenfassung; Ansprüche; Abbildungen ---	1,3
Y	US 4 605 820 A (C.M. CAMPBELL) 12. August 1986	1,3
A	siehe Zusammenfassung; Ansprüche; Abbildungen 1,2,8 ---	2
A	US 4 731 840 A (S.M. MNISZEWSKI) 15. März 1988 siehe Zusammenfassung; Abbildungen siehe Spalte 3, Zeile 44 - Spalte 5, Zeile 14 ---	1-4
	--- -/--	



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



**Siehe Anhang Patentfamilie**

<sup>3</sup> Besondere Kategorien von angegebenen Veröffentlichungen

**\*A\*** Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

\*E\* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L\* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

\*P\* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

**"Y"** Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

\*& Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

25. November 1998

Absendedatum des internationalen Rechercheberichts

02/12/1998

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

David, J

# INTERNATIONALER RECHERCHENBERICHT

In: itionales Aktenzeichen

PCT/EP 98/01269

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	W0 96 07994 A (BANKSYS) 14. März 1996 siehe Zusammenfassung; Ansprüche; Abbildung	1,2,4-7
A	GB 2 227 111 A (TOSHIBA) 18. Juli 1990	

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 98/01269

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR 2681165 A	12-03-1993	KEINE	
US 4605820 A	12-08-1986	KEINE	
US 4731840 A	15-03-1988	KEINE	
WO 9607994 A	14-03-1996	BE 1008699 A	02-07-1996
		AT 172805 T	15-11-1998
		AU 687622 B	26-02-1998
		AU 3377895 A	27-03-1996
		CA 2199504 A	14-03-1996
		EP 0780012 A	25-06-1997
		NO 971066 A	09-05-1997
GB 2227111 A	18-07-1990	JP 2187888 A	24-07-1990
		JP 2187785 A	23-07-1990
		FR 2641885 A	20-07-1990
		US 5293029 A	08-03-1994

